Highlights

- Highly-secure and flexible protection with predefined security policies and ability to easily define custom security policies.
- Provides a full suite of custom application gateways for popular Internet services for Windows NT.
- Simplifies management and minimizes human error through an industry leading graphical user interface and extensive on-line help.
- Provides on-site protection through comprehensive logs, and real-time alarms, evasive action; and provides strong user authentication.
- NCSA certified firewall for Windows NT.

Description

On-site computing is the new way to use computers to do business: simple, direct access to information and people no matter where you or they happen to be. It is simple because it uses standard web browsers to bring the universal Internet to your company’s Intranet. You can do real work from any location, and fast communication means having the competitive edge the competitive edge.

The growth of the Internet and the extension of intranets have increased security risks and introduced business problems. Many companies are asking important questions about using the Internet for business. How are hackers prevented from breaking in? How is network access controlled? How can airtight security be implemented without exhausting the budget?
The answer is on-site protection, the highest level of security, available with the NCSA-certified AltaVista firewall. Now you do not have to be on location to get on-site protection. AltaVista firewall manages the protection for you.

A firewall is a computer that monitors what comes into the network from the outside. This computer uses special firewall software to scan the information packets and allow only authorized users into the internal network. This protects the network from unwanted visitors and dangerous files from being passed through the firewall.

A firewall protects the systems and data on your network. In a case where a company’s security policies dictate how data must be protected, a firewall is very important since it embodies corporate policy. A firewall can act as your corporate interface to the Internet. Many corporations use their firewall systems as a place to store public information about corporate products and services, files to download, bug-fixes, and more.

Generally, firewalls are configured to protect against unauthenticated interactive log-ins from the outside world. Firewalls, more than any other function, help prevent unauthorized access to your network. Some firewalls permit only e-mail traffic through them. Others provide less strict protection, and block services that are known to be problems. More elaborate firewalls block traffic from the outside to the inside, but permit users on the inside to communicate freely with the outside.

Firewalls are also important since they can provide a single point where security and audits can be imposed.

Firewalls cannot protect against attacks that do not go through the firewall. For example, a magnetic tape can just as effectively be used to export data as a network. Allowing physical access to your firewall console is also extreme risky. Although separate software can be run on the firewall for virus detection, firewalls cannot offer complete protection against viruses entering via the desktop. Nor can a firewall protect against a data-driven attack which something is mailed or copied to an internal host where it is then executed.

A firewall can be used to secure a connection to a public network, or a connection to another private network within your organization (an intranet connection). The firewall performs the same functions in both cases. You may wish to deploy a firewall within a firewall, in which one firewall controls the connection to the Internet, and a second firewall controls connections between internal networks.

Any network connection involves a balance between security and availability of services. A firewall lets you control your network connection in three ways:

• Secure the internal network by preventing or restricting access to it.

• Enforce security policies for your site.

• Manage services that are available to internal users by controlling which hosts can access each service and what individuals can use them through the firewall.

The AltaVista Firewall deploys a combination of technologies that place highly-secure yet flexible barriers among your private networks, the Internet and other private networks. With AltaVista Firewall, you are in control, and have maximum security, real-time reporting, comprehensive logging, evasive action and an industry-leading graphical user interface. These features provide an unparalleled level of protection now available for Windows NT on Intel.

To use the Internet in place of a private network, each facility of an enterprise with LANs connects those LANs with a high-speed line to a local Internet Service Provider (ISP). The Internet then becomes the high-speed backbone of the enterprise, rather than costly private data circuits. The
result is a form of Virtual Private Networking (VPN) using the Internet rather than a private frame
relay or ATM network.

Enterprise LANs that are connected to the Internet typically have some form of firewall (packet fil-
ter, circuit, or application) technology to create a trusted administrative domain separate from the
Internet. A firewall regulates and logs interaction between trusted and untrusted networks. Local
policy decides what is allowed and denied. Many sites allow trusted users to initiate connections
to the Internet, but allow very restricted access from the Internet to their trusted network.

When building a VPN, policy is set with the firewall to allow the encrypted and authenticated
data from AltaVista tunnel clients into the trusted network. A combination of packet filtering and
forwarding relays on the firewall is used to pass tunnel traffic.

The tunneled data remains encrypted past the firewall and inside the trusted network until it
arrives at an AltaVista tunnel work group server. This server can be placed either on the same
LAN as the firewall or on a network LAN with special security requirements. For example, the
tunnel server may be on a LAN used for personnel, financial, or research data, and assures that
sensitive data does not pass in clear text across other parts of the enterprise. This gives the net-
work administrator the flexibility to maintain security within a semitrusted domain.

A personal password is used to guard against misuse of the PC, and an encryption key pair is used
to authenticate the specific PC with a specific trusted server. Authorization is based on a user
name, not an IP address, so users can roam and connect to different Internet access points and not
be tied to a specific address. No additional software is required inside the trusted network, since
normal routing is used once the packets are out of the tunnel and decrypted.

**Specifications**

<table>
<thead>
<tr>
<th>Characteristic</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows NT 4.0</td>
</tr>
<tr>
<td>Server or client workstation</td>
<td>Pentium 90 or higher</td>
</tr>
<tr>
<td>CD-ROM reader</td>
<td>Required for installation</td>
</tr>
<tr>
<td>Disk space</td>
<td>10 Mb for Windows NT</td>
</tr>
<tr>
<td>Memory</td>
<td>32 Mb</td>
</tr>
</tbody>
</table>

**Note:**
1. In general, the AltaVista tunnel enhances TCP/IP network transmissions with additional se-
curity and integrity. Thus, all the hardware and software (e.g., ethernet adapters and dialup net-
working) necessary to implement a TCP/IP networking environment should already be in place.
The tunnel requires no additional hardware or software besides the tunnel product itself.

**Nomenclature**

<table>
<thead>
<tr>
<th>Description</th>
<th>Nomenclature</th>
</tr>
</thead>
<tbody>
<tr>
<td>AltaVista firewall software license for 200 client nodes</td>
<td>S-PB-FRW-QB-55YAB-SC</td>
</tr>
</tbody>
</table>
Our worldwide staff of professionals is ready to meet your needs for process automation. For the location nearest you, please contact the appropriate regional office.

**AMERICAS**
29801 Euclid Avenue  
Wickliffe, Ohio USA 44092  
Telephone 1-216-585-8500  
Telefax 1-216-585-8756

**ASIA/PACIFIC**
152 Beach Road  
Gateway East #20-04  
Singapore 189721  
Telephone 65-391-0800  
Telefax 65-292-9011

**EUROPE, AFRICA, MIDDLE EAST**
Via Puccini 2  
16154 Genoa, Italy  
Telephone 39-10-6582-943  
Telefax 39-10-6582-941

**GERMANY**
Graefstrasse 97  
D-60487 Frankfurt Main  
Germany  
Telephone 49-69-799-0  
Telefax 49-69-799-2406